Information page for written examinations at Linköping University

Examination date	2018-03-15
Room (2)	G34(30) G36(17)
Time	14-18
Course code	TDDD17
Exam code	TEN2
Course name **Exam name**	Information Security, Second Course (Informationssäkerhet, fk) Written examination (En skriftlig tentamen)
Department	IDA
Number of questions in the examination	4
Teacher responsible/contact person during the exam time	Ulf Kargén
Contact number during the exam time	013-285876
Visit to the examination room approximately	15:00, 17:00
Name and contact details to the course administrator (name + phone nr + mail)	Madeleine Häger-Dahlqvist, 013-282360, madeleine.hager.dahlqvist@liu.se
Equipment permitted	Dictionary (printed, not electronic)
Other important information	Preliminary grading: C(3): 20 points, B(4): 26 points, A(5): 30 points
Number of exams in the bag	

LiTH, Linköpings tekniska högskola

IDA, Department of Computer and Information Science
Nahid Shahmehri

Written exam
TDDD17 Information Security
2018-03-15
14-18

Permissible aids
English dictionary (printed, NOT electronic)

Teacher on duty
Ulf Kargén, 013-285876

Instructions
There are 4 main questions on the exam. Your grade will depend on the total points you score. The maximum number of points is 34.

You may answer in Swedish or English.

Grading
The following grading scale is preliminary and might be adjusted during grading.

Grade	C (3)	B (4)	A (5)
Points required	20	26	30

1. System Security (10 points)

a) In a sentence or two, explain the concept Root of Trust. (1 points)

b) Explain the term *Measurement* in the context of TCG. Explain with figures and text how it works, the core hardware and/or software components involved, and give an example of what it can be used for. (4 points)

c) Back in the days of Windows XP, it was common for home PC users to always run with full Administrator privileges due to compatibility reasons. Which of Saltzer and Schroeder's 8 design principles does this violate? Name and explain the principle in a sentence or two. (1 point)

d) Explain how the above practice of running with full superuser privileges during day-to-day use can significantly increase the consequences of an attack against vulnerable software running on the PC, e.g. a web browser. (1 point)

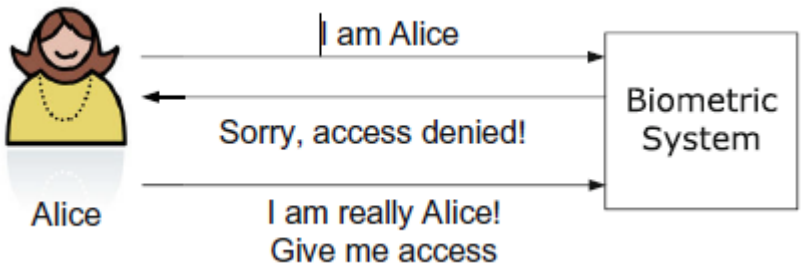
e) What is the principal difference between Mandatory Access Control (MAC) and Discretionary Access Control (DAC)? (1 point)

f) Explain in a sentence or two what sets *rootkits* apart from "regular" malware. (1 point)

g) A common rootkit technique is to load a malicious device driver. Explain the purpose of this and how it helps the rootkit achieve its goals. (1 point)

2. Identification and authentication, Biometric user authentication (8 points)

a) What type of security threat does the figure below describe? What are the effect for legitimate users of this security threat and what aspect of security is violated? (2 points)



b) Indicate briefly how attacks based on *probing* of tokens (smart cards, RFID devices etc) may be performed and mention at least one possible way of defending against probing! (2 points)

c) What makes universality, uniqueness, permanence and measurability (collectability) four important qualities when choosing a biometric trait? (4 points)

3. Network security (10 points)

a) Describe what “air-gaps” are and how those are useful for network security. Are those good/practical to have and what can breach those? (2 points)

b) List as many attacks typical for wireless networks as you can. Can you rely on typical coverage range of wireless networks as a security measure? (4 points)

c) Much of Internet security, especially e-commerce, is based on TLS/SSL. (4 points)

   i. What is the difference between those two?

   ii. What are certificates, how those are used and validated, what are possible problems?

   iii. Describe, in two sentences each, five basic attacks prevented by proper use of TLS/SSL

4. Database Security and Privacy (6 points)

a) Assume user Bob creates a table Student(Name, PN, Age) and, thereafter, the following 12 SQL commands are issued in the given order by the given users. Note that some of these commands will fail due to insufficient privileges. Identify all those commands that fail. (You only need to list the statement number of the statements that fail; there is no need for providing an explanation/justification).

```
# statement 1, issued by user Bob
GRANT SELECT, INSERT, DELETE ON Student TO Alice, Charlie WITH GRANT
OPTION;

# statement 2, issued by user Bob
INSERT INTO Student VALUES (“Alice”, 319, 21);

# statement 3, issued by user Bob
GRANT SELECT ON Student TO Eve;

# statement 4, issued by user Alice
SELECT Name FROM Student;

# statement 5, issued by user Alice
GRANT SELECT ON Student TO Eve, Charlie WITH GRANT OPTION;

# statement 6, issued by user Eve
GRANT SELECT ON Student TO Charlie;

# statement 7, issued by user Bob
REVOKE SELECT ON Student FROM Charlie;

# statement 8, issued by user Charlie
SELECT PN FROM Student;
```

statement 9, issued by user Bob
REVOKE SELECT, INSERT, DELETE ON Student FROM Alice;

statement 10, issued by user Charlie
GRANT SELECT ON Student TO Dave;

statement 11, issued by user Eve
SELECT PN FROM Student;

statement 12, issued by user Charlie
SELECT PN FROM Student WHERE Name="Alice";

b) Consider the following of security classes:

TopSecrect > *Secret* > *Confidential* > *Unclassified*

Suppose we have two tables, X and Y, where X has security class Secret and Y has security class Confidential. If user Bob wants to copy data from table Y into table X, which security class would he need a clearance for to be allowed such a copying under the Bell-LaPadula model. If multiple security classes would be possible, list every one of them. (You only need to list the security class(es); there is no need for providing an explanation/justification).

c) Consider the following two tables, E and T. Suppose attribute Disease in table T is a sensitive attribute and Age, Weight, and Postal Code are not sensitive, and table E represents some external data about all persons in the postal code area 291. Given this external data, list all quasi-identifiers of table T. Notice that there might be multiple different quasi-identifiers; if this is the case, you have to list all of them. (You only need to list the quasi-identifier(s); there is no need for providing an explanation/justification).

T

Age	**Weight**	**Postal Code**	**Disease**
19	70	311	Cold
19	71	291	Flu
18	72	483	Flu
18	71	291	Arthritis

E

Name	**Age**	**Weight**	**Postal Code**
Sven	19	70	291
Gustav	19	71	291
Bob	19	71	291
Dave	18	71	291

d) In which cases can a table be 5-anonymous but not 3-anonymous?

e) Recall that the definition of differential privacy is based on a notion of neighboring databases. Define this notion; i.e., when do we say that two databases D and D' are neighbors?

f) Assume a table with data about employees of a company including their salaries. Assume furthermore that the company has only three levels of salary: 35.000 SEK, 40.000 SEK, and 45.000 SEK (i.e., the salary of every employee is one of these amounts). Then, for each of the following two statistical queries, what is the sensitivity Δq of the query?
(You only need to provide the two numbers: sensitivity of Q1 and sensitivity of Q2; there is no need for providing an explanation/justification).

Q1: What is the number of employees who have the highest salary level (45.000 SEK)?

Q2: What is the sum of the salaries of all employees?